Symantec AntiVirus™ for Caching Integration Guide

Symantec AntiVirus™ for Caching Integration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.
Documentation version 4.3
PN: 10306121

Copyright Notice

Copyright © 2000-2004 Symantec Corporation.
All Rights Reserved.
Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.
NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.
No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. CarrierScan Server, Bloodhound, LiveUpdate, NAVEX, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation. Sun, Sun Microsystems, the Sun logo, StorEdge, Sun Enterprise, Java, Ultra, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc., in the United States and other countries. Microsoft, ActiveX, Windows, Windows NT, and the Windows Logo are registered trademarks of Microsoft Corporation in the United States and other countries. Red Hat is a registered trademark of Red Hat Software, Inc., in the United States and other countries. Linux is a registered trademark of Linus Torvalds. NetApp, Data ONTAP, NetCache, Network Appliance, and Web Filer are registered trademarks or trademarks of Network Appliance, Inc., in the United States and other countries. Blue Coat is a trademark of Blue Coat Systems, Inc., in the United States and other countries. Cisco is a registered trademark of Cisco Systems, Inc. Adobe, Acrobat, and Acrobat Reader are trademarks of Adobe Systems Incorporated. THIS PRODUCT IS NOT ENDORSED OR SPONSORED BY ADOBE SYSTEMS INCORPORATED, PUBLISHERS OF ADOBE ACROBAT.
Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.
A modified version of a freeware SNMP library is used in this software. This software is Copyright © 1988, 1989 by Carnegie Mellon University All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.
CMU software disclaimer: “CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.”
A set of Unicode handling libraries is used in this software. This software is Copyright (c) 1995-2002 International Business Machines Corporation and others. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.
IBM software disclaimer: “THE SOFTWARE IS PROVIDED ‘AS IS’, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.”
Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Technical support

Chapter 1 Introducing Symantec AntiVirus™ for Caching

About Symantec AntiVirus for Caching 9
Supported caching devices 9
Software components 10
How to use the Symantec AntiVirus for Caching documentation 10
About the Symantec AntiVirus Scan Engine Implementation Guide 11
About the Symantec AntiVirus for Caching Integration Guide 11
Why you need virus protection for Web proxy/caching 12
How the scan engine protects against viruses 13
About Symantec Security Response 13

Chapter 2 Configuring Symantec AntiVirus for Network Appliance™ NetCache®

Software components 15
How the Symantec AntiVirus Scan Engine works with the NetApp NetCache client 16
Scanning files for viruses 16
Handling of infected files 17
Alerting users when infected files cannot be repaired 18
Providing user comforting 18
Preparing for installation 18
Configuring the Symantec AntiVirus Scan Engine 19
Configuring ICAP-specific options 19
Enabling data trickle 21
How data trickle works 22
Warnings and limitations about data trickle 23
Specifying which file types to scan 23
Editing the ICAP access denied message 26
Configuring the NetApp NetCache client 27
Activating the NetApp ICAP license 28
Configuring the NetApp NetCache client to use ICAP 1.0 28

Configuring the NetApp NetCache client to use ICAP 0.95 31
Known issues with the NetApp NetCache 32

Chapter 3 Configuring Symantec AntiVirus for Blue Coat™ Security

Software components 34
How the Symantec AntiVirus Scan Engine works with the Blue Coat Security client 34
Scanning files for viruses 34
Handling of infected files 35
Alerting users when infected files cannot be repaired 35
Preparing for installation 36
Configuring the Symantec AntiVirus Scan Engine 36
Configuring ICAP-specific options 36
Specifying which file types to scan 39
Editing the ICAP access denied message 42
Configuring the Blue Coat Security appliance 42
Creating an ICAP service for the scan engine 43
Creating an ICAP cluster 44
Creating Web Content and Web Access Policies for virus scanning 45
Known issues with the Blue Coat Security appliance 46

Chapter 4 Configuring Symantec AntiVirus for Cisco® ACNS Content Engine

Software components 47
How the Symantec AntiVirus Scan Engine works with the Cisco ACNS Content Engine client 48
Scanning files for viruses 48
Handling of infected files 49
Alerting users when infected files cannot be repaired 49
Preparing for installation 50
Configuring the Symantec AntiVirus Scan Engine 50
Configuring ICAP-specific options 50
Specifying which file types to scan 52
Editing the ICAP access denied message 55
Configuring the Cisco ACNS Content Engine client 56
Known issues with the Cisco ACNS Content Engine 59

Index

Chapter 1

Introducing Symantec AntiVirus™ for Caching

This chapter includes the following topics:

- About Symantec AntiVirus for Caching
- How to use the Symantec AntiVirus for Caching documentation
- Why you need virus protection for Web proxy/caching

About Symantec AntiVirus for Caching

Symantec AntiVirus™ for Caching provides virus scanning and repair services for a number of caching devices. You can scan files for viruses automatically as they are accessed from the Web before they are sent to the requesting user and stored in a cache. When a virus is found in a file and the file is repaired, the clean file is stored and forwarded to the requesting user.

Supported caching devices

Symantec AntiVirus for Caching supports the following caching devices:

- Network Appliance™ NetCache®
- Blue Coat™ Security appliances
- Cisco® ACNS Content Engines

Software components

In most cases, adding virus scanning to a supported cache device requires installation and configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  The Symantec AntiVirus Scan Engine is included in the Symantec AntiVirus for Caching distribution package.
- Connector code that lets the caching device communicate with the Symantec AntiVirus Scan Engine
  The connector handles the communication between the scan engine and the caching device and interprets the results that are returned from the scan engine after scanning. In most cases, the connector code is developed by the manufacturer of the caching device. The connector code typically must be installed and configured on the caching device. (The connector code may be preinstalled by the manufacturer.)
  In some cases, no connector code is necessary. Communication with the scan engine is handled by the caching device, and any configuration options are available directly on the device.

How to use the Symantec AntiVirus for Caching documentation

To configure Symantec AntiVirus for Caching to work with one of the supported caching devices, you need the documentation that is included in the Symantec AntiVirus for Caching distribution package and the documentation that is provided by the manufacturer of the caching device.

The Symantec AntiVirus for Caching distribution package includes the following documents:

- *Symantec AntiVirus Scan Engine Implementation Guide*
- *Symantec AntiVirus for Caching Integration Guide*

Because the manufacturer of the caching device develops the connector code to integrate the Symantec AntiVirus Scan Engine, the manufacturer of the caching device also prepares and distributes the supporting documentation for the connector code. You must obtain the connector code and any supporting documentation from the manufacturer if it does not ship directly with the device.

About the Symantec AntiVirus Scan Engine Implementation Guide

Use the *Symantec AntiVirus Scan Engine Implementation Guide* as the primary guide for installing and configuring the Symantec AntiVirus Scan Engine. This guide contains information that you need to consider about all of the scan engine configuration options.

You also need to reference the *Symantec AntiVirus for Caching Integration Guide* for instructions on configuring the scan engine to work with a specific caching device.

About the Symantec AntiVirus for Caching Integration Guide

The *Symantec AntiVirus for Caching Integration Guide* includes a chapter for each supported caching device. Use the guidance and recommendations that are in the appropriate chapter of this guide, in conjunction with the manufacturer-prepared documentation, to implement virus scanning.

Each chapter in the *Symantec AntiVirus for Caching Integration Guide* includes the following information:

- General information on how antivirus scanning works in conjunction with the caching device
  Virus scanning functionality (for example, handling of infected files, timing of file scanning, logging of infections found) can differ depending on the capabilities of the caching device and the complexity of the connector code. This section provides an overview of how the Symantec AntiVirus Scan Engine and the caching device interact during virus scanning.
- Information on configuring the scan engine to work with the caching device
  This section discusses the configuration options on the scan engine that must be configured to work with the caching device and may highlight other options that are important in setting up comprehensive virus protection. This information does not replace the information that is in the *Symantec AntiVirus Scan Engine Implementation Guide*. Consult the implementation guide for installation information and for additional information on configuring the Symantec AntiVirus Scan Engine to meet your needs.

- Information on configuring the caching device to work with the scan engine
  This section discusses any configuration options on the caching device that must be configured to work with the Symantec AntiVirus Scan Engine and may make recommendations for configuring the caching device to ensure comprehensive virus protection. This information does not replace the documentation that is provided by the manufacturer of the caching device. Consult the product documentation for additional information on configuring the caching device for virus scanning.
- Known issues
  This section describes issues that can affect operation between the Symantec AntiVirus Scan Engine and the caching device.

Why you need virus protection for Web proxy/ caching

The HTTP gateway is an underprotected area of most networks. Corporate security efforts have heavily focused on more traditional areas through which viruses can enter. Enterprises typically have focused security around known viruses that enter the network through more common means, such as CD-ROM or email, so hackers now exploit the Web as a means to enter corporate networks. Many new threats target port 80, which is usually open on corporate firewalls so that users can browse the Web.

Dedicated virus scanning for Web traffic is recommended for the following reasons:

- Scanning Web traffic lets you catch and block threats at the gateway, rather than multiple times at each desktop. Users can potentially disable desktop protection, which can leave your network vulnerable to attack.
- Because many people now use Web-based email, email-born viruses that would otherwise be caught by antivirus scanning at the SMTP gateway can slip through to infect the network.
- The industry trend has been to Web-enable many application environments to include the use of technologies like ActiveX, JavaScript, and Java applets to enhance the user experience. Many new threats are associated with these Web technologies. Malicious mobile code viruses, such as Nimda and Code Red, have entered networks as executables (for example, ActiveX, JavaScript, or Visual Basic Scripts) that appear to be part of safe Web content.

- Once a threat has been cached, malicious code can potentially be passed to other users on the network, which can compromise additional computers and data on the network.
- Malicious code can result in lost, stolen, or corrupted files, which can result in costly downtime to the enterprise.

How the scan engine protects against viruses

The Symantec AntiVirus Scan Engine detects viruses, worms, and Trojan horses in all major file types (for example, Windows files, DOS files, and Microsoft Word and Excel files). The Symantec AntiVirus Scan Engine includes a decomposer that handles most compressed and archive file formats and nested levels of files. You can configure the scan engine to limit scanning to certain file types based on file extension.

The Symantec AntiVirus Scan Engine provides protection against container files that can cause denial of service attacks (for example, container files that are overly large, that contain large numbers of embedded compressed files, or that have been designed to use resources maliciously and degrade performance). You can specify the maximum amount of time that the scan engine devotes to decomposing a file and its contents, the maximum file size for container files, and the maximum number of nested levels to be decomposed for scanning.

The Symantec AntiVirus Scan Engine also detects mobile code such as Java™, ActiveX®, and stand-alone script-based threats. The Symantec AntiVirus Scan Engine uses Symantec antivirus technologies, including Bloodhound™, for heuristic detection of new or unknown viruses; NAVEX™, which provides protection from new classes of viruses automatically through LiveUpdate; and Striker, for the detection of polymorphic viruses.

About Symantec Security Response

The Symantec AntiVirus Scan Engine is supported by the Symantec Security Response team. These Symantec engineers work 24 hours per day, 7 days per week, tracking new virus outbreaks and identifying new virus threats.

For more information about protection against a specific virus, visit the Symantec Security Response Web site at:

http://securityresponse.symantec.com

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Chapter 2

Configuring Symantec AntiVirus for Network Appliance™ NetCache®

This chapter includes the following topics:

- Software components
- How the Symantec AntiVirus Scan Engine works with the NetApp NetCache client
- Preparing for installation
- Configuring the Symantec AntiVirus Scan Engine
- Configuring the NetApp NetCache client
- Known issues with the NetApp NetCache

Software components

Symantec AntiVirus™ for Caching provides virus scanning and repair capabilities for Network Appliance™ (NetApp®) NetCache® appliances that use version 5.2.1R1 or later of the NetCache software.

Adding antivirus scanning to the NetApp NetCache requires configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

- The NetApp NetCache
  Some options are configured directly on the NetApp NetCache. No additional code is necessary to connect the Symantec AntiVirus Scan Engine to the NetApp NetCache.

How the Symantec AntiVirus Scan Engine works with the NetApp NetCache client

The NetApp NetCache is a caching proxy server. As the NetApp NetCache retrieves requested information from the Web, it also caches a copy of the information (stores a copy on disk). Where possible, it serves multiple requests for the same Web content from the cache.

NetApp NetCache clients use the Internet Content Adaptation Protocol (ICAP) to communicate with the Symantec AntiVirus Scan Engine. Clients can request virus scanning and repair as a file is retrieved from the Web before it is sent to the requesting user. When a virus is found in a downloaded file and the file is repaired, the clean file is cached and forwarded to the requesting user.

Symantec AntiVirus for Caching provides virus scanning and repair capabilities for any NetApp NetCache that uses version 5.2.1R1 or later of the NetCache software. The Symantec AntiVirus Scan Engine supports both the proprietary 0.95 implementation of ICAP and ICAP version 1.0, as presented in RFC 3507 (April 2003). The Symantec AntiVirus Scan Engine determines which version is appropriate for each request based on the header data that is provided by the NetApp NetCache when it contacts the Symantec AntiVirus Scan Engine to scan a file.

Scanning files for viruses

The manner in which the Symantec AntiVirus Scan Engine determines whether to scan a file differs depending on which version of ICAP is used.

For ICAP 0.95, when the Symantec AntiVirus Scan Engine is contacted by the NetApp NetCache to scan a file, a small amount of data from the file is transferred to the Symantec AntiVirus Scan Engine. (The number of bytes of data that is transferred is configured through the NetCache interface.) This data contains the file name, the HTTP header, and the first few bytes of the file to be scanned. The Symantec AntiVirus Scan Engine examines this data to determine whether to scan the file.

The Symantec AntiVirus Scan Engine first identifies the extension of the file to be scanned and then compares the extension to a list of extensions that are configured on the scan engine. If the file extension is one that the scan engine is

configured to scan, or if the scan engine is configured to scan all files, the Symantec AntiVirus Scan Engine requests the remainder of the file from the NetApp NetCache client and scans it.

If the scan engine is not configured to scan the file extension or does not recognize the file extension, the Symantec AntiVirus Scan Engine examines the first few bytes of the file's contents to determine whether the file could contain a virus. Based on this examination, the scan engine might scan a file even when the extension is not listed in the extension list.

ICAP 1.0 lets the Symantec AntiVirus Scan Engine provide information to the NetApp NetCache client on which file types are to be scanned based on the scan engine configuration. Based on this information, the NetApp NetCache client forwards either the entire file to the scan engine for scanning (if the file extension is one that was identified for scanning) or the first few bytes of the file to the scan engine for preview (if the file extension is unknown or is not one that was identified for scanning). The scan engine examines the first few bytes of the file to determine whether the file could contain a virus. Based on this examination, the scan engine might request and scan a file even when it is not identified for scanning.

See "Specifying which file types to scan" on page 23.

Handling of infected files

You configure how to handle infected files through the Symantec AntiVirus Scan Engine administrative interface. When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following:

- Scan only: Scan files for viruses, but do nothing to infected files.
- Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair.
- Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files).
- Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.

Alerting users when infected files cannot be repaired

Access to a file is blocked when an unrepairable virus is found or a policy violation occurs. The Symantec AntiVirus Scan Engine supplies an HTML text message to display when a requested file is blocked. The default HTML text file indicates that access is denied because the file contained an unrepairable virus or because a policy violation occurred. You can customize the text that is displayed by editing this file or by substituting an alternate file.

See "Editing the ICAP access denied message" on page 26.

Providing user comforting

When a user attempts to download an extremely large or complex file from the Internet, antivirus scanning can cause a delay during which the requesting browser (and thus the user) receives no feedback on the progress of the download. The data trickle feature lets you provide users with a quicker download response and avoid potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete.

Warning: Using the data trickle feature can compromise antivirus integrity. Before enabling this feature, ensure that you have evaluated all of the risks.

See "Enabling data trickle" on page 21.

Preparing for installation

To interface with the Symantec AntiVirus Scan Engine, the NetApp NetCache must use version 5.2.1R1 or later of the NetCache software to support ICAP version 0.95 or 1.0. Before you install the scan engine, ensure that the NetApp NetCache meets this requirement.

The Symantec AntiVirus Scan Engine cannot be installed on the NetCache appliance. The scan engine must be installed on another computer on the network. Ensure that the computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure both the scan engine and the NetApp NetCache.

Configuring the Symantec AntiVirus Scan Engine

The scan engine must be configured to use ICAP as the communication protocol. At installation, ICAP is the default communication protocol. If the scan engine is configured to use another protocol, you can change the protocol to ICAP through the scan engine administrative interface. You must configure several ICAP-specific options.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Configuring ICAP-specific options

After you install the Symantec AntiVirus Scan Engine, you must configure several settings that are specific to ICAP.

Table 2-1 describes the protocol-specific options for ICAP.

Table 2-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by entering the appropriate bind address.
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number greater than 1024 that is not in use by any other program or service.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains an unrepairable virus or violates a policy that you have established. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you edit the existing file, you do not have to change this setting. See "Editing the ICAP access denied message" on page 26.

Table 2-1 Protocol-specific options for ICAP

Option	Description
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Scan files for viruses, but do nothing to infected files. ■ Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair. ■ Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files). ■ Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.
Data trickle	When a user attempts to download an extremely large or complex file from the Internet, antivirus scanning can cause a delay during which the requesting browser (and thus the user) receives no feedback on the progress of the download. You can use the data trickle feature to provide users with a quicker download response and avoid potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete. See "Enabling data trickle" on page 21.

To configure ICAP-specific options

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.
   The configuration settings are displayed for the selected protocol.
3. Under ICAP Protocol Configuration, in the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
4. In the Port number box, type the TCP/IP port number that the NetApp NetCache client uses to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.

5 In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.

6 In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.

The default setting is Scan and repair or delete. If you plan to use the data trickle feature, you must select Scan only.

7 Click **Confirm Changes** to save the configuration.

8 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- You must stop and restart the service manually if you have changed the communication protocol from RPC to ICAP through the administrative interface (rather than selecting ICAP at installation).
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Enabling data trickle

When a user attempts to download an extremely large or complex file from the Internet, a period of time elapses while antivirus scanning takes place during which the browser (and thus the user) receives no feedback on the progress of the download. Without feedback, the user might try to click the browser Refresh button even though the download is working properly. In some instances, the browser can time out while waiting for the scan to complete.

The data trickle feature provides users with a quicker download response and avoids potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete.

Data trickling is available for versions 0.95 and 1.0 of ICAP. The ICAP scan policy must be set to Scan only when data trickle is enabled. (When you enable data trickle, the ICAP scan policy is automatically reset to Scan only.) In the Scan only configuration, infected files cannot be deleted or repaired.

Warning: Using the data trickle feature can compromise antivirus integrity. Before enabling this feature, ensure that you have evaluated all of the risks.

See "Warnings and limitations about data trickle" on page 23.

To enable data trickle

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, check **Enable Trickle**.
   Data trickling is disabled by default.
3. In the Trickle timeout box, type the number of seconds that the scan process will run before data trickling begins.
   Data trickling does not start if scanning is complete before the trickle time-out elapses. The default setting is 5 seconds. The maximum setting is 86,400 seconds (24 hours).
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

How data trickle works

When a user downloads a file, the Symantec AntiVirus Scan Engine stores a copy of the requested file in a buffer and begins the scanning process. While the copy is being scanned, a small portion of the original, unscanned file is sent to the user through the client application. The trickled data triggers the File Download or Save File As dialog box, which provides the user with a quicker download response.

After the user enters a file location and saves the file, the file is trickled to the user in small amounts at regular intervals until the scan is complete to prevent the browser from timing out. The browser indicates how much of the file has been trickled.

If no virus is detected during the scan, data trickling stops, and the remainder of the file is sent to the user.

If a virus is detected, data trickling stops, and no additional data is sent to the user. The user receives no notification that the file might be incomplete or that it might contain a virus. Symantec AntiVirus Scan Engine logging regarding virus detection functions normally during data trickling. A log message about the virus detection is sent to all active logging destinations.

Note: Data trickling is not used during scanning of POST transaction data.

Warnings and limitations about data trickle

Enabling data trickle can compromise antivirus integrity. Data trickling is not recommended for the following reasons:

- The data that is trickled to the user might contain a virus.
  If you enable data trickle, you should install an antivirus program such as Symantec AntiVirus Corporate Edition that provides real-time virus scanning. If the trickled data is infected, the real-time virus scanning feature will detect the virus immediately.
- For FTP downloads that use optimizers, when a broken connection is detected, the optimizer resumes the download from the point at which the disconnection occurred. This results in downloading the remainder of the file and possibly reconstructing an infected file.
- ICAP requires that a return code message be included in the first line of the file header. When data trickling begins, the ICAP return code 200 (OK) is embedded in the trickled data file. Because the file has not been scanned, this message might be inaccurate. The trickled data file might contain a virus.
- When data trickling is enabled, the ICAP scan policy is set to Scan only. You cannot configure your scanning policy to repair or delete infected files when data trickle is enabled.
- The user receives no notification that the trickled data file is incomplete or infected.

Specifying which file types to scan

You control which files are scanned by the Symantec AntiVirus Scan Engine by using either an inclusion or an exclusion list, or you can scan all files regardless of extension. The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in a prepopulated

exclusion list. The default exclusion list contains those file types that are unlikely to contain viruses. You can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those file types that are specifically listed in an inclusion list are scanned. Thus, with an inclusion list, there is an almost limitless number of possible file extensions that are not scanned. For this reason, the inclusion list is not prepopulated, but you can choose to populate this list.

If you use either the inclusion or the exclusion list to control the file types that are scanned (rather than scanning all files), the manner in which the list is applied differs depending on which version of ICAP that you use.

The scan engine handles inclusion and exclusion lists in one of the following ways:

- ICAP version 1.0: The inclusion or exclusion list is used by the Symantec AntiVirus Scan Engine to determine which files to scan of those that are embedded in archival file formats (for example, .zip or .lzh files). All top-level files that are sent to the scan engine are scanned regardless of file extension.
- ICAP version 0.95: The inclusion or exclusion list applies to all files that are sent to the Symantec AntiVirus Scan Engine for scanning. The extension list is referenced for both top-level files and embedded files that are contained in archival file formats (for example, .zip or .lzh files).

Note: Exclusion and inclusion lists do not scan all file types. Thus, new types of viruses might not always be detected. Scanning all files regardless of extension is the most secure setting, but imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the exclusion or inclusion list.

Specify which file types to scan

You can control which file types are scanned by specifying extensions that you want to include or exclude from scanning, or you can scan all files regardless of extension.

To scan all files except for those with extensions that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.

3 Edit the exclusion list to add extensions that you do not want to scan or to delete extensions that you want to scan.
Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 To restore the default extension list, click **Restore default lists**.

5 Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan only files with extensions that are in the inclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.

3 Edit the inclusion list to add extensions that you want to scan or to delete extensions that you do not want to scan.
Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan all files regardless of extension

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.

3 Click **Confirm Changes** to save the configuration.

4 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Editing the ICAP access denied message

Access to a file is blocked when the file contains a virus that cannot be repaired or when the file violates a policy that you have configured. The Symantec AntiVirus Scan Engine passes an HTML text message to the NetApp NetCache to display to the user when the requested file is blocked.

You can customize the message that is displayed in one of the following ways:

- Specify an alternate HTML file.
  See "Configuring ICAP-specific options" on page 19.
- Edit the ICAP access denied HTML file.

Table 2-2 describes the default text that is in the ICAP access denied message.

Table 2-2 Default text for ICAP access denied message

Default text	Description
The content you just requested had a problem and was blocked by the Symantec AntiVirus Scan Engine based on local administrator settings. Contact your local administrator for further information.	Text that is in the symcsinf.htm file, which is displayed to the user when a requested file contains a virus and cannot be repaired or when the file violates a policy that you have configured.

To edit the ICAP access denied message

1. Locate the Symantec AntiVirus Scan Engine ICAP access denied HTML file and open it with a text editor.
   For Solaris and Linux, the default location and file name of the HTML file is /opt/SYMCScan/etc/symcsinf.htm. For Windows 2000 Server/Server 2003, the default location and file name of the file is C:\Program Files\Symantec\Scan Engine\SYMCSINF.htm.
2. Make your changes to the file.
3. Save the file.
4. Stop and restart the Symantec AntiVirus Scan Engine.

Configuring the NetApp NetCache client

Each NetApp NetCache client must be configured to work with the Symantec AntiVirus Scan Engine. Each NetApp NetCache should be configured in accordance with the Network Appliance documentation and should be installed and working properly before you submit files for scanning.

Supported NetApp NetCache appliances must use version 5.2.1R1 or later of the NetCache software to work with the Symantec AntiVirus Scan Engine. Configuration of the NetCache client differs depending on which version of ICAP that you are using.

See “Configuring the NetApp NetCache client to use ICAP 1.0” on page 28.

See “Configuring the NetApp NetCache client to use ICAP 0.95” on page 31.

To use either version of ICAP, you must first activate the ICAP feature on the NetApp NetCache using the license key that is supplied by Network Appliance.

Activating the NetApp ICAP license

To use either version of ICAP with the Symantec AntiVirus Scan Engine, you must activate the ICAP feature on the NetApp NetCache with a license. Network Appliance, Inc. has provided the license key, QIMCZIE, to Symantec Corporation. This license is valid through June 27, 2006, and is approved for use by all Symantec AntiVirus Scan Engine customers.

To activate the NetApp ICAP license

1. On the Setup tab, in the menu on the left, click **System > Licenses**.
2. On the System Licenses page, in the ICAP license box, type the following license key:
   QIMCZIE
3. Click **Commit Changes**.

Configuring the NetApp NetCache client to use ICAP 1.0

Each NetApp NetCache client must be configured to use ICAP 1.0 to communicate with the Symantec AntiVirus Scan Engine. NetApp NetCache clients should be configured in accordance with the Network Appliance documentation.

Configure the NetApp NetCache client to use ICAP 1.0

To configure the NetApp NetCache client to use ICAP 1.0, you must do the following:

- Activate the ICAP 1.0 license on the NetApp NetCache if you have not already done so.
  See "Activating the NetApp ICAP license" on page 28.
- Enable ICAP 1.0.
- Add two service farms for the Symantec AntiVirus Scan Engine, one for scanning of inbound traffic and one for scanning of outbound traffic (POST transactions).

To enable ICAP 1.0

1. Access the NetCache console by opening the following URL:
   http://<netcacheIP:port>
   where <netcacheIP:port> is the IP address and port number for the NetApp NetCache.
2. Log on to the NetCache console.

3 On the Setup tab, in the menu on the left, click **ICAP**, and then click **ICAP 1.0**.

4 On the General tab, check **Enable ICAP Version 1.0**.

5 Click **Commit Changes**.
Activate the NetApp ICAP 1.0 license on the NetApp NetCache if you have not already done so. An error message displays if you have not installed the ICAP license key.
See "Activating the NetApp ICAP license" on page 28.

To add a service farm for scanning of inbound traffic

1 Access the NetCache console by opening the following URL:
http://<netcacheIP:port>
where <netcacheIP:port> is the IP address and port number for the NetApp NetCache.

2 Log on to the NetCache console.

3 On the Setup tab, in the menu on the left, click **ICAP**, and then click **ICAP 1.0**.

4 On the Service Farms tab, click **New Service Farm**.

5 In the Service Farm Name box, type a name for the new service farm.

6 In the Vectoring Point list, click **RESPMOD_PRECACHE**.

7 Check **Service Farm Enable**.

8 In the Load Balancing list, click **Least Usage Based**.

9 Ensure that the Bypass on Failure check box is not checked.

10 In the Consistency list, click **Strong**.

11 Ensure that the lbw Threshold box is empty.

12 In the Services box, type the ICAP URL string for the Symantec AntiVirus Scan Engine that will provide scanning services for inbound traffic.
Use the following format:
icap://<scanengineIP:port>/avscanresp on
where <scanengineIP:port> is the IP address and port number on which the Symantec AntiVirus Scan Engine listens.

13 On the ACL tab, check **Enable Access Control Lists**.

14 In the HTTP ACL box, identify the access control list for the new service farm.
Use the following format:
icap<servicefarmname> any
where <servicefarmname> is the name of the new service farm for scanning of inbound traffic.

15 On the Service Farm tab, in the list of current ICAP service farms, in the Enable column, click the check box for the new service farm.

16 Click **Commit Changes**.

To add a service farm for scanning of outbound traffic

1 Access the NetCache console by opening the following URL:
http://<netcacheIP:port>
where <netcacheIP:port> is the IP address and port number for the NetApp NetCache.

2 Log on to the NetCache console.

3 On the Setup tab, in the menu on the left, click **ICAP**, and then click **ICAP 1.0**.

4 On the Service Farms tab, click **New Service Farm**.

5 In the Service Farm Name box, type the name of the new service farm.

6 In the Vectoring Point list, click **REQMOD_PRECACHE**.

7 Check **Service Farm Enable**.

8 In the Load Balancing list, click **Least Usage Based**.

9 Ensure that the Bypass on Failure check box is not checked.

10 In the Consistency list, click **Strong**.

11 Ensure that the lbw Threshold box is empty.

12 In the Services box, type the ICAP URL string for the Symantec AntiVirus Scan Engine that will provide scanning services for outbound traffic.
Use the following format:
icap://<scanengineIP:port>/avscanreq on
where <scanengineIP:port> is the IP address and port number on which the Symantec AntiVirus Scan Engine listens.

13 On the ACL tab, check **Enable Access Control Lists**.

14 In the HTTP ACL box, identify the access control list for the new service farm.
Use the following format:
icap<servicefarmname> any
where <servicefarmname> is the name of the new service farm for scanning of outbound traffic.

15 On the Service Farm tab, in the list of current ICAP service farms, in the Enable column, click the check box for the new service farm.

16 Click **Commit Changes**.

Configuring the NetApp NetCache client to use ICAP 0.95

You configure the NetApp NetCache client to work with the scan engine as follows:

- The port number that is configured for the Symantec AntiVirus Scan Engine must match the ICAP URL port number that is provided to the NetApp NetCache client.
- The configured prefix size for the number of bytes that are passed to the Symantec AntiVirus Scan Engine to determine whether a file should be scanned must be set to 4 bytes (under ICAP URL Arguments).
  In cases in which the Symantec AntiVirus Scan Engine does not recognize the file extension, the scan engine examines this prefix information to determine whether to scan the entire file.
- The NetApp ICAP license must be activated on the NetApp NetCache so that you can use ICAP.
  See "Activating the NetApp ICAP license" on page 28.
- The ICAP settings on the NetApp NetCache client must be configured according to the guidelines in Table 2-3.

Table 2-3 ICAP 0.95 settings on the NetApp NetCache client

Setting	Recommended value
ICAP 0.95 Enable	On
ICAP Service Type	Respmod
ICAP URL IP address	<Symantec AntiVirus Scan Engine IP address>
ICAP URL port number	1344
ICAP URL Arguments	/respmod?preview =4

Known issues with the NetApp NetCache

The NetApp NetCache might time out while waiting for a reply from the Symantec AntiVirus Scan Engine when extremely large or complex files are being scanned. When a scan request times out, the NetApp NetCache returns a garbled HTTP message to the requesting browser. You cannot adjust the time-out threshold on the NetApp NetCache.

Chapter 3

Configuring Symantec AntiVirus for Blue Coat™ Security

This chapter includes the following topics:

- Software components
- How the Symantec AntiVirus Scan Engine works with the Blue Coat Security client
- Preparing for installation
- Configuring the Symantec AntiVirus Scan Engine
- Configuring the Blue Coat Security appliance
- Known issues with the Blue Coat Security appliance

Software components

Symantec AntiVirus™ for Caching provides integrated virus scanning and repair capabilities for Blue Coat™ Security appliances that support the Internet Content Adaptation Protocol (ICAP).

Adding virus scanning to a Blue Coat Security appliance requires installation and configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  The Symantec AntiVirus Scan Engine is included in the Symantec AntiVirus for Caching distribution package.
  See "Configuring the Symantec AntiVirus Scan Engine" on page 36.
- The Blue Coat Web Content Policy (for incoming HTTP traffic) and the Web Access Policy (for outgoing HTTP traffic) for virus scanning
  See "Configuring the Blue Coat Security appliance" on page 42.

How the Symantec AntiVirus Scan Engine works with the Blue Coat Security client

The Blue Coat Security appliance handles all of the HTTP traffic on your network. As the Blue Coat Security appliance retrieves requested information from the Web, it also caches (stores a copy on disk) the information. When possible, it serves multiple requests for the same Web content from the cache.

Blue Coat Security clients use ICAP to communicate with the Symantec AntiVirus Scan Engine. The clients request virus scanning as a file is retrieved from the Web before it is sent to the requesting user. When a virus is found in a downloaded file and the file is repaired, the clean file is cached and forwarded to the requesting user. When a virus is found that cannot be repaired, access to the infected file is denied.

You can use a single Symantec AntiVirus Scan Engine to support a Blue Coat Security client, or you can use multiple scan engines to handle larger scan volumes. To use multiple scan engines, you must create an ICAP service cluster on the Blue Coat Security client. Load balancing is handled automatically through the cluster configuration.

Scanning files for viruses

When the Symantec AntiVirus Scan Engine receives a scanning request from the Blue Coat Security client, a small amount of data from the file is transferred to the Symantec AntiVirus Scan Engine. This data contains the first 4 bytes of

the file to be scanned. The Symantec AntiVirus Scan Engine examines this data to determine whether to scan the file.

If the file extension is one that should be scanned, the Symantec AntiVirus Scan Engine requests the remainder of the file from the Blue Coat Security client and scans it. Depending on the examination of the first 4 bytes, the scan engine might request and scan a file even when it is not identified for scanning.

If the file is a container file and contains embedded files, the Symantec AntiVirus Scan Engine extracts the embedded files from the container file and scans the files with extensions that match those that are specified for scanning. When scanning is complete, the container file is reassembled. Infected files that are embedded in the container file can be repaired or deleted, depending on how the scan engine is configured to handle infected files.

Handling of infected files

You configure how to handle infected files through the Symantec AntiVirus Scan Engine administrative interface. When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following:

- Scan only: Scan files for viruses, but do nothing to infected files.
- Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair.
- Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files).
- Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.

Alerting users when infected files cannot be repaired

Access to a file is blocked when an unrepairable virus is found or a policy violation occurs. The Symantec AntiVirus Scan Engine supplies an HTML text message to display when a requested file is blocked. The default HTML text file indicates that access is denied because the file contained an unrepairable virus or because a policy violation occurred. You can customize the text that is displayed by editing this file or by substituting an alternate file.

See "Editing the ICAP access denied message" on page 42.

Preparing for installation

To interface with the Symantec AntiVirus Scan Engine, the Blue Coat Security appliance must be ICAP-enabled for ICAP version 1.0, as presented in RFC 3507 (April 2003). Blue Coat Security appliances that are running SG2.1.06 or later meet this requirement.

The Symantec AntiVirus Scan Engine cannot be installed on the Blue Coat Security appliance. The scan engine must be installed on another computer on the network. Ensure that the computer on which you plan to install the Symantec AntiVirus Scan Engine meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure both the scan engine and the Blue Coat Security appliance.

See "Configuring the Symantec AntiVirus Scan Engine" on page 36.

See "Configuring the Blue Coat Security appliance" on page 42.

Configuring the Symantec AntiVirus Scan Engine

The scan engine must be configured to use ICAP as the communication protocol. At installation, ICAP is the default communication protocol. If the scan engine is configured to use another protocol, you can change the protocol to ICAP through the scan engine administrative interface. You must configure several ICAP-specific options.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Configuring ICAP-specific options

After you install the Symantec AntiVirus Scan Engine, you must configure several settings that are specific to ICAP.

Table 3-1 describes the protocol-specific options for ICAP.

Table 3-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.

Table 3-1 Protocol-specific options for ICAP

Option	Description
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains an urepairable virus or violates a policy that you have established. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you edit the existing file, you do not have to change this setting. See "Editing the ICAP access denied message" on page 42.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Deny access to the infected file, but do nothing to the infected file. ■ Scan and delete: Delete all infected files without attempting repair. ■ Scan and repair files: Attempt to repair infected files and deny access to unrepairable files (but do not delete files that cannot be repaired from archive files). ■ Scan and repair or delete: Attempt to repair infected files, and delete any unrepairable files from archive files.
Data trickle	When a user attempts to download an extremely large or complex file from the Internet, antivirus scanning can cause a delay during which the requesting browser (and thus the user) receives no feedback on the progress of the download. You can use the data trickle feature to provide users with a quicker download response and avoid potential session time-out errors. When data trickle is enabled, the requested file is sent (trickled) to the user in small amounts at regular intervals until the scan is complete. **Note:** To prevent redundancy, you should use the Blue Coat Security patience page feature instead of data trickle. Data trickle is disabled by default on the Symantec AntiVirus Scan Engine. For more information about Blue Coat Security's patience page feature, see the appropriate Blue Coat Security documentation.

To configure ICAP-specific options

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.
2. On the Protocol tab, click **ICAP**.
   The configuration settings display for the selected protocol.
3. In the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
4. In the Port number box, type the TCP/IP port number to be used by the Blue Coat Security client to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.
5. In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.
6. In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete.
7. Verify that the Enable Trickle box is not checked.
   Data trickling is disabled by default.
   For more information about how data trickle works, warnings, and limitations, see the *Symantec AntiVirus Scan Engine Implementation Guide*.
8. Click **Confirm Changes** to save the configuration.
9. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Specifying which file types to scan

To specify the types of files to be scanned for viruses, you must configure settings on both the Blue Coat Security client and the Symantec AntiVirus Scan Engine.

The Blue Coat Security client makes an initial determination, based on MIME type or file extension, about whether to pass a file to the Symantec AntiVirus Scan Engine for scanning. You configure which files are passed to the Symantec AntiVirus Scan Engine for scanning when you set up the Web Content Policy for virus scanning on the Blue Coat Security client. The recommended setting is to configure the Blue Coat Security client to pass all files to the Symantec AntiVirus Scan Engine for virus scanning.

See "Creating Web Content and Web Access Policies for virus scanning" on page 45.

The Symantec AntiVirus Scan Engine also must be configured to scan selected file types. The scan policy on the Symantec AntiVirus Scan Engine is as important as the Blue Coat Security policy because it is used after the scan engine receives a file from the Blue Coat Security client to determine which files to scan of those that are contained in archive or container file formats.

You can control which embedded files are scanned by specifying on the Symantec AntiVirus Scan Engine the extensions that you do not want to scan (using an exclusion list) or by specifying extensions that you want to scan (using an inclusion list), or you can scan all file types regardless of extension.

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in a prepopulated exclusion list. This is the recommended setting. The default exclusion list contains file types that are unlikely to contain viruses, but you can edit this list.

Using an inclusion list to control which types of files are scanned is the least secure setting. Only those files types that are listed in an inclusion list are scanned; therefore, with an inclusion list, there is an almost limitless number of possible file extensions that are not scanned. For this reason, the inclusion list is not prepopulated, but you can populate this list if you want to limit the file types that are scanned.

Note: Inclusion and exclusion lists do not scan all file types. Thus, new types of viruses might not always be detected. Scanning all files regardless of extension is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you might want to scan all files even if you normally control the file types that are scanned with the inclusion or exclusion list.

Specify which file types to scan

You can scan all files regardless of extension on the Symantec AntiVirus Scan Engine, or you can control which file types are scanned by specifying extensions that you want to include or exclude from scanning.

To scan all files regardless of extension

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.
3. Click **Confirm Changes** to save the configuration.
4. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

To scan all files except for those with extensions that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
3. Edit the extension list to add extensions that you do not want to scan or delete extensions that you want to scan.
   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.
4. To restore the default extension list, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan only files with extensions that are in the inclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.

3 Edit the extension list to add extensions that you want to scan or delete extensions that you do not want to scan.
Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the current UI session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Editing the ICAP access denied message

Access to a file is blocked when the file contains a virus that cannot be repaired or when the file violates a policy that you have configured. The Symantec AntiVirus Scan Engine passes an HTML text message to the Blue Coat Security client to display to the user when the requested file is blocked.

You can customize the message that is displayed in one of the following ways:

- Specify an alternate HTML file.
  See "Configuring ICAP-specific options" on page 36.
- Edit the ICAP access denied HTML file.

Table 3-2 describes the default text that is in the ICAP access denied message.

Table 3-2 Default text for ICAP access denied message

Default text	Description
The content you just requested had a problem and was blocked by the Symantec AntiVirus Scan Engine based on local administrator settings. Contact your local administrator for further information.	Text that is in the symcsinf.htm file, which is displayed to the user when a requested file contains a virus and cannot be repaired or when the file violates a policy that you have configured.

To edit the ICAP access denied message

1. Locate the Symantec AntiVirus Scan Engine ICAP access denied HTML file and open it with a text editor.
   For Solaris and Linux, the default location and file name of the HTML file is /opt/SYMCScan/etc/symcsinf.htm. For Windows 2000 Server/Server 2003, the default location and file name of the file is C:\Program Files\Symantec\Scan Engine\SYMCSINF.htm.
2. Make your changes to the file.
3. Save the file.
4. Stop and restart the Symantec AntiVirus Scan Engine.

Configuring the Blue Coat Security appliance

To interface with the scan engine, the Blue Coat Security appliance must be ICAP-enabled for ICAP version 1.0 and must be running SG2.1.06 or later. The Blue Coat Security appliance should be configured in accordance with the appropriate Blue Coat documentation and should be functioning properly before integrating virus scanning.

To integrate virus scanning on the Blue Coat Security appliance, you do the following (using the Blue Coat Management Console or in command-line mode):

- Create new ICAP services for incoming and outgoing HTTP traffic for each Symantec AntiVirus Scan Engine.
  If you are using multiple Symantec AntiVirus Scan Engines, repeat this step for each scan engine.
  See "Creating an ICAP service for the scan engine" on page 43.
- Create a separate ICAP cluster for incoming and outgoing traffic and add the appropriate scan engine ICAP services to the cluster.

  Note: This step is only applicable if you plan to use multiple scan engines to support virus scanning.

  See "Creating an ICAP cluster" on page 44.
- Create a Web Content Policy (for incoming HTTP traffic) and a Web Access Policy (for outgoing HTTP traffic) for virus scanning, and configure the scan engine ICAP service or cluster as the virus scanner.
  See "Creating Web Content and Web Access Policies for virus scanning" on page 45.

Creating an ICAP service for the scan engine

You must create and configure an ICAP service for both incoming and outgoing traffic for each Symantec AntiVirus Scan Engine. If you are using multiple scan engines to support virus scanning, you must do the same for each scan engine.

For more information, see the Blue Coat Security appliance documentation.

Table 3-3 shows the recommended settings for configuring the ICAP service on the Blue Coat Security appliance.

Table 3-3 ICAP service settings

Management Console setting	Recommended value
ICAP version	1.0
Service URL	For incoming HTTP traffic, use: icap://<scanengineservername>/avscanresp For outgoing HTTP traffic (POST transactions), use: icap://<scanengineservername>/avscanreq
Vendor for ICAP service	Symantec You must select Symantec to ensure proper functionality.

Table 3-3 ICAP service settings

Management Console setting	Recommended value
Maximum number of connections	128 The maximum number that should be used for this setting is 256 scan threads. This number should be the same as or close to the maximum number of threads that is selected on the Symantec AntiVirus Scan Engine. See "Editing the ICAP access denied message" on page 42.
Connection timeout (seconds)	180 The default setting of 70 seconds does not allow sufficient time for the Symantec AntiVirus Scan Engine to decompose and scan all of the embedded files in larger archive and container file formats. This setting should match the maximum extract time that is selected on the Symantec AntiVirus Scan Engine for container file processing limits. The default setting on the scan engine is 180 seconds.
Patience page	Enabled Enabling the patience page prevents a connection time-out from occurring while the requesting Web browser waits for the Symantec AntiVirus Scan Engine to decompose and scan large files. The default setting is 10 seconds.
Method supported	For incoming HTTP traffic, use: Response modification For outgoing HTTP traffic (POST transactions), use: Request modification
Preview size	4 bytes **Note:** To ensure proper functionality for virus scanning, you must set the preview size to 4 bytes. Virus scanning will not occur when any other value is used for this setting.

Creating an ICAP cluster

If you are using multiple scan engines to handle larger scan volumes, you must create a separate ICAP service cluster for incoming and outgoing traffic. You also must add the appropriate ICAP services into the cluster configuration.

For incoming traffic, the cluster must contain the defined scan engine ICAP services that support the Response modification method. For outgoing traffic (to provide scanning for POST transactions), the cluster must contain the defined scan engine ICAP services that support the Request modification method. The Blue Coat Security appliance will not let you create a cluster that contains ICAP services that support different methods.

Select the cluster as the virus scanner (rather than an individual scan engine) when you set up your Web Content and Web Access Policies. In this way, load balancing is handled automatically through the cluster configuration. You can create the ICAP service cluster using the Blue Coat Security appliance Management Console or the Blue Coat command-line mode.

For more information, see the Blue Coat Security appliance documentation.

Creating Web Content and Web Access Policies for virus scanning

You must create a Web Content Policy on the Blue Coat Security appliance for virus scanning and configure the scan engine ICAP service or cluster as the virus scanner for that policy.

For more information, see the Blue Coat Security appliance documentation.

When you configure the Web Content and Web Access Policies for virus scanning, you must specify the following information:

- Which file types or MIME types to pass to the Symantec AntiVirus Scan Engine for virus scanning
  For maximum security, the recommended setting is to configure the Blue Coat Security client to pass all files to the Symantec AntiVirus Scan Engine for virus scanning. This lets the scan engine determine which files can contain viruses and scan accordingly, based on the examination of the first 4 bytes of each file.

  Note: Only the top-level file is examined by the Blue Coat Security client. Container and archive files can contain additional files that should be scanned for viruses. The list of file types sent to the Symantec AntiVirus Scan Engine for scanning should include archive and container file types.

- The ICAP service or cluster that will perform the scanning
  Select the ICAP service or the ICAP cluster that you created for the Symantec AntiVirus Scan Engine.

- The manner in which files are handled when the scan engine is unavailable for any reason or an error is generated when scanning a file
  For maximum security, the recommended setting is Deny the request. (Depending on the version of Blue Coat Security that you are running, this setting might be called Fail Closed.) Selecting Deny the request (or Fail Closed) denies access to a file when the file has not been scanned. Selecting Bypass ICAP service (or Fail Open) lets unscanned files pass through when the scan engine is unavailable for any reason or an error is generated during a scan.

Known issues with the Blue Coat Security appliance

The Blue Coat Security appliance might time out while waiting for a reply from the Symantec AntiVirus Scan Engine when extremely large or complex files are being scanned.

If the Patience Page setting is enabled on the Blue Coat Security appliance and a scan request times out, the user receives no notification that a time-out occurred, and the Patience Page refreshes indefinitely. If the Patience Page setting is not enabled and a scan request times out, the Blue Coat Security appliance sends an ICAP communication error to the browser.

The likelihood of a time-out can be decreased by increasing the connection time-out setting to the recommended value (180 seconds) on the Blue Coat Security appliance.

Chapter 4

Configuring Symantec AntiVirus for Cisco® ACNS Content Engine

This chapter includes the following topics:

- Software components
- How the Symantec AntiVirus Scan Engine works with the Cisco ACNS Content Engine client
- Preparing for installation
- Configuring the Symantec AntiVirus Scan Engine
- Configuring the Cisco ACNS Content Engine client
- Known issues with the Cisco ACNS Content Engine

Software components

Symantec AntiVirus™ for Caching provides antivirus scanning and repair services for the Cisco® Application and Content Networking System (ACNS) Content Engine version 5.1.5.

Adding antivirus scanning to the Cisco ACNS Content Engine requires configuration of the following components:

- The Symantec AntiVirus Scan Engine, which provides the virus scanning and repair services
  For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

- Cisco ACNS Content Engine
  ICAP services must be configured to route files to the Symantec AntiVirus Scan Engine for scanning.
  See "Configuring the Cisco ACNS Content Engine client" on page 56.

How the Symantec AntiVirus Scan Engine works with the Cisco ACNS Content Engine client

The Cisco ACNS software provides an integrated caching and content-delivery platform that is designed to help improve operations and reduce costs to enterprises and service providers that are hosting managed enterprise content delivery networks. The ACNS software can be deployed to optimize WAN bandwidth, accelerate deployment of Web applications, and add Web content security.

The Cisco ACNS Content Engine uses the Internet Content Adaptation Protocol (ICAP) to communicate with the Symantec AntiVirus Scan Engine to request virus scanning. You can use a single Symantec AntiVirus Scan Engine to support a Cisco ACNS Content Engine client, or you can use multiple scan engines to handle larger scan volumes. To use multiple scan engines, you can create an ICAP service that contains multiple scan engines and select the type of load balancing that you want to use.

Scanning files for viruses

When the Symantec AntiVirus Scan Engine receives a scanning request from the Cisco ACNS Content Engine, a small amount of data from the file is transferred to the Symantec AntiVirus Scan Engine. This data contains the first 4 bytes of the file to be scanned.

The Symantec AntiVirus Scan Engine examines this data to determine whether to scan the file. If the file extension is one that should be scanned, the Symantec AntiVirus Scan Engine requests the remainder of the file from the Cisco ACNS Content Engine and scans it. Depending on the examination of the first 4 bytes, the scan engine might request and scan a file even when it is not identified for scanning.

See "Specifying which file types to scan" on page 52.

If the file is a container file and contains embedded files, the Symantec AntiVirus Scan Engine extracts the embedded files from the container file and scans the files that have extensions that match those that are specified for scanning. When scanning is complete, the container file is reassembled. Infected files that are embedded in the container file can be repaired or deleted, depending on how the scan engine is configured to handle infected files.

Handling of infected files

You configure how to handle infected files through the Symantec AntiVirus Scan Engine administrative interface. When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following:

- Scan only: Scan files for viruses, but do nothing to infected files.
- Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair.
- Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files).
- Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.

Note: Container files (for example, .zip files) can contain both clean and infected embedded files. When an infected file that cannot be repaired is embedded in a container file, the entire container file and its contents is treated as an infected file unless you have chosen to delete infected files (by selecting either scan and delete or scan and repair or delete).

Alerting users when infected files cannot be repaired

Access to a file is blocked when an unrepairable virus is found or a policy violation occurs. The Symantec AntiVirus Scan Engine supplies an HTML text message to display when a requested file is blocked. The default HTML text file indicates that access is denied because the file contained an unrepairable virus or because a policy violation occurred. You can customize the text that is displayed by editing this file or by substituting an alternate file.

See "Editing the ICAP access denied message" on page 55.

Preparing for installation

To interface with the Symantec AntiVirus Scan Engine, you must be running version 5.1.5 or later of the Cisco ACNS software. The Cisco ACNS Content Engine must be installed and working properly before you attempt to activate virus scanning.

The Symantec AntiVirus Scan Engine must be installed on a computer on the network that meets the system requirements that are listed in the *Symantec AntiVirus Scan Engine Implementation Guide*.

After you have installed the Symantec AntiVirus Scan Engine, you must configure both the scan engine and the Cisco ACNS Content Engine.

See "Configuring the Symantec AntiVirus Scan Engine" on page 50.

See "Configuring the Cisco ACNS Content Engine client" on page 56.

Configuring the Symantec AntiVirus Scan Engine

The scan engine must be configured to use ICAP as the communication protocol. At installation, ICAP is the default communication protocol. If the scan engine is configured to use another protocol, you can change the protocol to ICAP through the scan engine administrative interface. You must configure several ICAP-specific options.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Configuring ICAP-specific options

After you install the Symantec AntiVirus Scan Engine, you must configure several settings that are specific to ICAP.

Table 4-1 describes the protocol-specific options for ICAP.

Table 4-1 Protocol-specific options for ICAP

Option	Description
Scan engine bind address	By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.

Table 4-1 Protocol-specific options for ICAP

Option	Description
Port number	The port number must be exclusive to the Symantec AntiVirus Scan Engine. For ICAP, the default port number is 1344. If you change the port number, use a number that is greater than 1024 that is not in use by any other program or service.
HTML message displayed for infected files	The Symantec AntiVirus Scan Engine includes a default HTML message to display to users when access to a file is denied because it contains an urepairable virus or violates a policy that you have established. You can customize this message by specifying an alternate path and file name or by editing the existing file. If you edit the existing file, you do not have to change this setting. See "Editing the ICAP access denied message" on page 55.
ICAP scan policy	When an infected file is found, the Symantec AntiVirus Scan Engine can do any of the following: ■ Scan only: Scan files for viruses, but do nothing to infected files. ■ Scan and delete: Scan files for viruses, and delete any infected files that are embedded in archive or container files without attempting repair. ■ Scan and repair files: Attempt to repair infected files, but do nothing to unrepairable files (that is, do not delete the files from archive or container files). ■ Scan and repair or delete: Attempt to repair infected files, and delete unrepairable files from archive or container files.
Data trickle	This setting is not functional for Symantec AntiVirus for Cisco ACNS Content Engine. Do not change this setting from the default (off).

To configure ICAP-specific options

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Configuration**.

2 On the Protocol tab, click **ICAP**.
The configuration settings display for the selected protocol.

3. In the Scan Engine bind address box, type a bind address, if necessary.
   By default, the Symantec AntiVirus Scan Engine binds to all interfaces. You can restrict access to a specific interface by typing the appropriate bind address.
4. In the Port number box, type the TCP/IP port number to be used by the Cisco ACNS Content Engine to pass files to the Symantec AntiVirus Scan Engine for scanning.
   The default setting for ICAP is port 1344.
5. In the HTML message displayed for infected files box, type the path and file name to supply an alternate HTML file, if necessary.
6. In the ICAP scan policy list, select how you want the Symantec AntiVirus Scan Engine to handle infected files.
   The default setting is Scan and repair or delete.
7. Verify that the Enable Trickle box is not checked.
   Data trickling is disabled by default.
8. Click **Confirm Changes** to save the configuration.
9. Do one of the following:
   - Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
     If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
   - Click **Restart** to save your changes and restart the scan engine service now.
   - Click **Save/No Restart** to save your changes.
     Changes will not take effect until the service is restarted.

Specifying which file types to scan

Viruses are found only in file types that contain executable code. You can save bandwidth and time by limiting the files to be scanned to only those file types that can contain viruses. You can specify the types of files that are scanned for viruses though the Symantec AntiVirus Scan Engine interface. You can control which file types are scanned by using an inclusion list or an exclusion list, or you can scan all file types regardless of extension.

When the scan engine receives a file from the Cisco ACNS Content Engine, the Symantec AntiVirus Scan Engine examines a small amount of data to determine whether to scan the file. If the file extension is one that should be scanned, the scan engine scans the file. This procedure is followed for each file, including

those that are contained in archive or container file formats. Depending on the examination of the first 4 bytes, the scan engine might request and scan a file even when it is not identified for scanning.

The Symantec AntiVirus Scan Engine is configured by default to scan all files except those with extensions that are listed in a prepopulated exclusion list. The default exclusion list contains those file types that are unlikely to contain viruses. You can customize this list.

Note: Inclusion and exclusion lists do not scan all file types. Therefore, new types of viruses might not always be detected. Scanning all files regardless of extension is the most secure setting, but it imposes the heaviest demand on resources. During virus outbreaks, you may want to scan all files even if you normally control the file types that are scanned with an inclusion or exclusion list.

For more information, see the *Symantec AntiVirus Scan Engine Implementation Guide*.

Specify which file types to scan

You can control which file types are scanned by specifying the file extensions that you want to include or exclude from scanning, or you can scan all file types regardless of extension.

To scan all files except those with extensions that are in the exclusion list

1. On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.
2. On the AntiVirus tab, under File types to be scanned, click **Scan all files except those with the following extensions**.
   This is the recommended setting.
3. Edit the exclusion list to add extensions that you do not want to scan or to delete extensions that you want to scan.
   Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To exclude files with no extension, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.
4. To restore the default extension list, click **Restore default lists**.
5. Click **Confirm Changes** to save the configuration.

6 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan only files with extensions that are in the inclusion list

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, check **Scan files with the following extensions**.

3 Edit the inclusion list to add extensions that you want to scan or to delete extensions that you do not want to scan.
  Use a period with each extension in the list. Separate each extension with a semicolon (for example, .com;.doc;.bat). To scan files that have no extensions, use two adjacent semicolons (for example, .com;.exe;;). Use a question mark (?) as a wildcard character to match a single character.

4 Click **Confirm Changes** to save the configuration.

5 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

To scan all files regardless of extension

1 On the Symantec AntiVirus Scan Engine administrative interface, in the left pane, click **Blocking Policy**.

2 On the AntiVirus tab, under File types to be scanned, click **Scan all files regardless of extension**.

3 Click **Confirm Changes** to save the configuration.

4 Do one of the following:

- Click **Continue** to make additional changes to the Symantec AntiVirus Scan Engine configuration.
  If you click Continue and the session times out before you save your changes by clicking Restart or Save/No Restart, your changes will be lost.
- Click **Restart** to save your changes and restart the scan engine service now.
- Click **Save/No Restart** to save your changes.
  Changes will not take effect until the service is restarted.

Editing the ICAP access denied message

Access to a file is blocked when the file contains a virus that cannot be repaired or when the file violates a policy that you have configured. The Symantec AntiVirus Scan Engine passes an HTML text message to the Cisco ACNS Content Engine to display to the user when the requested file is blocked.

You can customize the message that is displayed in one of the following ways:

- Specify an alternate HTML file.
  See "Configuring ICAP-specific options" on page 50.
- Edit the ICAP access denied HTML file.

Table 4-2 describes the default text that is in the ICAP access denied message.

Table 4-2 Default text for ICAP access denied message

Default text	Description
The content you just requested had a problem and was blocked by the Symantec AntiVirus Scan Engine based on local administrator settings. Contact your local administrator for further information.	Text that is in the symcsinf.htm file, which is displayed to the user when a requested file contains a virus and cannot be repaired or when the file violates a policy that you have configured.

To edit the ICAP access denied message

1. Locate the Symantec AntiVirus Scan Engine ICAP access denied HTML file and open it with a text editor.
   For Solaris and Linux, the default location and file name of the HTML file is /opt/SYMCScan/etc/symcsinf.htm. For Windows 2000 Server/Server 2003, the default location and file name of the file is C:\Program Files\Symantec\Scan Engine\SYMCSINF.htm.
2. Make your changes to the file.
3. Save the file.
4. Stop and restart the Symantec AntiVirus Scan Engine.

Configuring the Cisco ACNS Content Engine client

To integrate virus scanning for the Cisco ACNS Content Engine, you must create ICAP services for the Symantec AntiVirus Scan Engine. The options for antivirus protection on the Cisco ACNS Content Engine are configured through the command-line interface.

For more information, see the Cisco documentation for configuring ICAP services for the ACNS Content Engine.

The virus scan functionality for the Cisco ACNS Content Engine should be configured in accordance with the Cisco documentation and the supplemental guidance in Table 4-3.

Table 4-3 ICAP Service configuration settings

Setting	Description
Rules and access control lists	Ensure that the Symantec AntiVirus Scan Engine ICAP process (virus scanning) applies to all Web traffic on your network so that all files are scanned for viruses. If you use a complex configuration with many access control lists or rules-templates for your ICAP processes, you may inadvertently let some files pass through without being scanned. To ensure that all Web traffic on your network is scanned for viruses, when you configure the Cisco ACNS Content Engine to pass files to the Symantec AntiVirus Scan Engine for scanning, use the following command: icap apply all

Table 4-3 ICAP Service configuration settings

Setting	Description
Vector point	Designate the position for both request and response mode within the request flow in which the Symantec AntiVirus Scan Engine ICAP service (virus scanning) should start. Client requests are vectored to the ICAP service where they are modified (scanned) before being returned. Create an avscanreq service to provide REQMOD processing and an avscanresp service to provide RESPMOD processing. ICAP vector points include the following: ■ REQMOD_PRECACHE and REQMOD_POSTCACHE These vector points modify a request before the request is sent to the origin server. ■ RESPMOD_PRECACHE This vector point modifies the request as it is sent from the origin server before it is stored in the cache. **Note:** Virus scanning services are configured as RESPMOD_PRECACHE or REQMOD_PRECACHE so that infected objects are not cached.
Error handling	Indicate whether to allow (bypass) or deny (return-error) access to a file when virus scanning fails for any reason. The default setting is bypass. If you are configuring the Symantec AntiVirus Scan Engine ICAP service through the command line and you want to deny access to files that have not been scanned, add the following line to the service configuration: error-handling return-error **Note:** Selecting bypass (which allows access to files that have not been scanned for viruses) can leave your network vulnerable to virus attacks.

Table 4-3 ICAP Service configuration settings

Setting	Description
Rescan cache	Indicate whether to rescan cached objects by updating the ISTag when virus definitions change. When the ISTag updates, previously cached responses are resubmitted for virus scanning before being forwarded to a requesting user. Rescanning cached objects when the ISTag changes ensures that your network is protected against new threats as soon as possible. Objects are stored in the cache after they have been scanned for viruses and have been determined to be clean. Virus definitions, which are used by the scan engine to detect viruses, are updated periodically to protect against new viruses. It is possible that newly updated virus definitions may detect a virus that was previously undetected in a cached object. To rescan cached objects when the ISTag changes, add the following line to the service configuration: icap rescan-cache ISTag-change **Note:** This setting is global and affects all defined ICAP services.
Server time-out	Specify the maximum amount of time (in seconds) for the Cisco ACNS Content Engine to wait for a scan to finish before closing the connection with the scan engine. If no response is received from the scan engine in the specified amount of time, the procedure for Error Handling applies. The default setting is 120 seconds. To avoid tying up resources, this setting should match or slightly exceed the maximum extract time that is specified for container files on the Symantec AntiVirus Scan Engine. Certain container files with many nested levels of files can take longer to scan. The default setting on the scan engine is 180 seconds. To change the server time-out setting to the recommended setting (180 seconds), use the following command: tcp server-rw-timeout 180

Table 4-3 ICAP Service configuration settings

Setting	Description
Bypass requests	Indicate whether to bypass ICAP processing for selected media. Streaming media requests (requests from Windows, Real Media, and QuickTime media players) cannot be scanned for viruses, so ICAP processing must be bypassed for these types of requests. ICAP processing of streaming media requests is turned off by default. Do not change the default setting. **Note:** This setting is global and affects all defined ICAP services.

Known issues with the Cisco ACNS Content Engine

The following are known issues with the Cisco ACNS Content Engine:

- When virus scanning fails for any reason, the setting for error handling applies. The default setting for error handling on the Cisco ACNS Content Engine software is to bypass the ICAP Service. This lets the file pass through without being scanned, which leaves your network vulnerable to virus attack.
  If you do not define error handling in your ICAP service configuration, the default setting (Bypass) is applied automatically. To deny access to unscanned files, you must specify Return-error by adding the following line to your ICAP service configuration:
  error-handling return-error
- You configure the maximum amount of time that the Content Engine waits for a scan to finish before it closes the connection with the scan engine. If no response is received from the scan engine in the specified amount of time and you have specified Return-error for error handling, the Content Engine displays an error message to the requesting user.
  The text of the error message indicates that the requested file is not available because of a problem with the Symantec AntiVirus Scan Engine. The error message is misleading because a time-out can be caused by factors other than the scan engine.
- You configure the persistent connection period on the Cisco ACNS Content Engine. The persistent connection period specifies how long the Cisco ACNS Content Engine keeps a connection open to receive data from the scan engine if a transmission has not completed.
  The default setting is 600 seconds. To avoid tying up resources, the recommended value is 185 seconds.

- When the Symantec AntiVirus Scan Engine is installed on a Web server or file server on your network, content that is stored on that server is not scanned for viruses.

  Do not install the Symantec AntiVirus Scan Engine on a Web server or file server that contains content that will be accessed from your network.

- The Cisco ACNS Content Engine imposes a maximum file size for uploaded files. This maximum file size is not configurable.

  When a user attempts to upload a file that exceeds the maximum file size, the browser returns a time-out error. The error message does not indicate the cause of the time-out. The ICAP log entry indicates that the maximum file size for uploaded files was exceeded.

Index

A

antivirus scanning 13

B

Blue Coat Security
- configuring for virus scanning 42
- configuring scan engine 36
- creating an ICAP cluster 44
- creating an ICAP service 43
- creating Web content/access policies 45
- ICAP access denied message 42
- known issues 46
- overview of virus scanning 34
- software components 34
- specifying files to scan 39
- system requirements 36
- user notification of infection found 35

C

Cisco ACNS Content Engine
- configuring for virus scanning 56
- configuring scan engine 50
- ICAP access denied message 55
- known issues 59
- overview of virus scanning 48
- software components 47
- specifying files to scan 52
- system requirements 50
- user notification of infection found 49

D

data trickle, NetApp NetCache
- description 18
- implementing 21
- warnings and limitations 23

F

files to be scanned
- Blue Coat Security 39

files to be scanned *(continued)*
- Cisco ACNS Content Engine 52
- NetApp NetCache 23

I

ICAP access denied message
- Blue Coat Security 42
- Cisco ACNS Content Engine 55
- default text 27
- NetApp NetCache 26

N

NetApp NetCache
- configuring for virus scanning 27
- configuring scan engine 19
- ICAP 0.95 configuration 31
- ICAP 1.0 configuration 28
- ICAP access denied message 26
- ICAP license 28
- known issues 32
- overview of virus scanning 16
- software components 15
- specifying files to scan 23
- system requirements 18
- user notification of infection found 18

notification, of infection found
- Blue Coat Security 35
- Cisco ACNS Content Engine 49
- NetApp NetCache 18

S

software components
- Blue Coat Security 34
- Cisco ACNS Content Engine 47
- NetApp NetCache 15

Symantec AntiVirus for Caching
- documentation 10
- software components 10
- supported devices 9

Symantec AntiVirus Scan Engine
configuring for Blue Coat Security 36
configuring for Cisco ACNS Content Engine 50
configuring for NetApp NetCache 19
documentation 11
virus protection 13

V

virus protection
description 13
for Web proxy/caching 12